

# Notice of Allowability

Application No.

10/090,422

Examiner

Eleni A. Shiferaw

Applicant(s)

PAATERO, LAURI

Art Unit

2136

## -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to RCE.
2. ☒ The allowed claim(s) is/are 1-17, 20-23, 25-46, 49-52, 54-57, 60 and 62-66.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

### Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date 12/4/07.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

12,10,07

#### DETAILED ACTION

1. An examiner initiated interview has been made, on December 4, 2007 with Andrew T. Hyman, to resolve typo problems, 112 antecedent bases, and moving dependent claims to the base claims and the applicant's undersigned attorney Andrew T. Hyman approved all the changes examiner suggested on December 7, 2007.

#### EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Andrew T. Hyman on December 7, 2007.

3. Claims 1, 29, 30, 54, 60, 65, 66 are amended and claims 18, 19, 47, 48, 61, and 67, are cancelled as follows:

1. (Currently Amended) A method comprising:  
having an identity authenticated in a first system;  
a second system causing a key to be generated for use in the second system;  
the second system generating a certificate for the key; and

establishing the identity of ~~[[the]]~~ a user in the second system by signing the certificate for the key using the authenticated identity of the user in the first system,

wherein the certificate for the key for use in the second system contains usage limitations, including a temporal limit on usage,

wherein the temporal limit requires that once a secure socket layer session on the second system is completed, the certificate or a corresponding key is destroyed, ~~[[and]]~~

wherein said usage limitations also include a limit on use of said key for encryption only, which excludes use of said key for signature verification ~~[[.]]~~ ; and

wherein the first system is a wireless communication system and wherein the second system is a computer connected to an Internet.

18. (Canceled)

19. (Canceled)

29. (Currently Amended) A method comprising:

generating a key for use in a network environment by a user having an authenticated identity not associated with said network environment;

generating a certificate for the key; and

establishing the identity of the user in said network environment by signing the certificate for the key using the user's authenticated identity,

wherein the certificate for the key for use in the network environment contains usage limitations, including a temporal limit on usage,

wherein the temporal limit requires that once a secure socket layer session on the second system is completed, the certificate or a corresponding key is destroyed, [[and]]

wherein said usage limitations also include a limit on use of said key for encryption only, which excludes use of said key for signature verification [[.]] : and

wherein the first system is a wireless communication system and wherein the second system is a computer connected to an Internet.

30. (Currently Amended) A system comprising:

a device forming part of a second system, the device having means for causing a key to be generated for use in the second system by a user having an authenticated identity in a first system,

said device of the second system having means for generating a certificate for the key;  
and

a second device forming part of the first system, the second device having means for storing information regarding the authenticated identity of the user in the first system,

said second device further having means for communicating said information; and

wherein the device of the second system has means for receipt of said information from the second device, and further has means for establishing the identity of the user in the second system by signing the certificate for the key using the authenticated identity of the user in the first system,

wherein the certificate for the key for use in the second system contains usage limitations, including a temporal limit on usage,

wherein the temporal limit requires that once a secure socket layer session on the second system is completed, the certificate or a corresponding key is destroyed, [[and]]

wherein said usage limitations also include a limit on use of said key for encryption only, which excludes use of said key for signature verification [[.]] ; and

wherein the first system is a wireless communication system and wherein the second system is a computer connected to an Internet.

47. (Canceled)

48. (Canceled)

54. (Currently Amended) A system as defined in claim [[53]] 30, wherein one usage limitation is that a third party of the second system should accept the key for use in the second system only for certain types of operations.

60. (Currently Amended) A wireless device comprising:

means for storing information regarding an authenticated identity of a user in a first system associated with the wireless device;

means for receipt of a certificate from a second device that is part of a second system, the certificate being for a key that is for use in the second system; and

means for establishing the identity of the user in the second system by signing the certificate using the authenticated identity of the user in the first system and transferring the signed certificate to the device of the second system wherein the certificate for the key for use in the second system contains usage limitations, including a temporal limit on usage,

wherein the temporal limit requires that once a secure socket layer session on the second system is completed, the certificate or a corresponding key is destroyed,

wherein said usage limitations also include a limit on use of said key for encryption only, which excludes use of said key for signature verification [[.]] ;

wherein the second device includes means for generating the key to be used in said second system; and

wherein the first system is a wireless communication system and wherein the second system is a computer connected to an Internet.

61. (Canceled)

65. (Currently Amended) A program stored on a computer readable medium for execution by a processor, the program having code for:

generating a key for use in a network environment by a user having an authenticated identity not associated with said network environment;

generating a certificate for the key; and

establishing the identity of the user in said network environment by signing the certificate for the key using the user's authenticated identity.

wherein the certificate for the key for use in the network environment contains usage limitations, including a temporal limit on usage,

wherein the temporal limit requires that once a secure socket layer session on the second system is completed, the certificate or a corresponding key is destroyed, [[and]]

wherein said usage limitations also include a limit on use of said key for encryption only, which excludes use of said key for signature verification ; and

wherein the first system is a wireless communication system and wherein the second system is a computer connected to an Internet.

66. (Currently Amended) A wireless device comprising:

storage module configured to store information regarding an authenticated identity of a user in a first system associated with the wireless device;

receiving module, configured to receive a certificate from a second device that is part of a second system, the certificate being for a key that is for use in the second system; and

signing module configured to establish the identity of the user in the second system by signing the certificate using the authenticated identity of the user in the first system and transferring the signed certificate to the device of the second system,

wherein the certificate for the key for use in the second system contains usage limitations, including a temporal limit on usage,

wherein the temporal limit requires that once a secure socket layer session on the second system is completed, the certificate or a corresponding key is destroyed, [[and]]

wherein said usage limitations also include a limit on use of said key for encryption only, which excludes use of said key for signature verification [[.]] ; and

wherein the second device includes a generating module configured to generate the key to be used in said second system, and

wherein the first system is a wireless communication system and wherein the second system is a computer connected to an Internet.

67. (Canceled)

***Allowable Subject Matter***

4. Claims 1-17, 20-23, 25-46, 49-52, 54-57, and 60, 62-66 are allowed.

The following is a statement of reasons for the indication of allowable subject matter:

Applied references either alone or in combination fail to teach a method/system comprising having an identity authenticated in a wireless communication system, a computer causing a key to be generated for use in the computer, generates a certificate for the key, and signs the certificate for the key using the authenticated identity of the user in the wireless communication system, wherein the certificate for the key for use in the second system contains usage limitations, including a temporal limit on usage, wherein the temporal limit requires that once a secure socket layer session on the second system is completed, the certificate or a corresponding



key is destroyed, wherein said usage limitations also include a limit on use of said key for encryption only, which excludes use of said key for signature verification.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

#### *Conclusion*

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number:  
10/090,422  
Art Unit: 2136

Page 10

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

December 9, 2007

  
12/10/07